Oracle® Communications Services Gatekeeper

Release Notes

Release 6.1

E64631-03

June 2017

ORACLE®

Oracle Communications Services Gatekeeper Release Notes, Release 6.1

E64631-03

Contents

2 Database Schema Changes

Preface

This book includes information about this release of Oracle Communications Services Gatekeeper.

Audience

This book is intended for all Services Gatekeeper users.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For related information, see the following Services Gatekeeper documents:

- *Oracle Communications Services Gatekeeper Concepts*
- *Oracle Communications Services Gatekeeper Getting Started Guide*
- *Oracle Communications Services Gatekeeper Multi-tier Installation Guide*

1

Release Notes

This document lists the new, enhanced, and removed features, resolved and known issues, documentation notes, and documentation updates for release 6.1 of Oracle Communications Services Gatekeeper.

This chapter contains the following sections:

Software Upgrades

This section lists the software upgrades to the this release of Services Gatekeeper.

New Support for Running Services Gatekeeper on Oracle Linux 7.2

New in this release, Services Gatekeeper is now supported to run on Oracle 7.2 (64-bit).

New Support for Virtual Platforms

This release of Services Gatekeeper is supported to run on these virtual platforms:

- VMware ESXi 5.5
- Oracle Virtual Machine 3.2.9

New Support for Oracle 12 RAC

Services Gatekeeper now supports the Oracle 12c RAC database, which now appears as an option in the installation GUI.

New Support for Oracle 12c CDB and PDB

Services Gatekeeper now supports the Container Database (CDB) and Pluggable Database (PDB) versions of the Oracle 12c database.

Installing on Single Tier Implementation

The only thing you need to change when using the Oracle 12c CDB and PDB features with Single Tier implementations is that you should enter the PDB Service Name when you install Services Gatekeeper:

- GUI Installation - On the Database Information installation screen, after you select **Oracle** database, you are offered the choice of entering an **SID**, or a PDB **Service Name**. Select the **Service Name** radio button and enter the service name that your PDB implementation uses.
- Silent Installation - Enter the correct database service name in the **DATABASE_SERVICE_NAME** item, and ensure that **DATABASE_SID_SELECTED** is set to **false**

Installing on Multi Tier Implementations

The Oracle 12c CDB and Oracle 12c PDB databases installations require different settings as explained in these sections:

- Oracle 12c CDB Database (and other non-PDB databases) - Use these datasources:
  - For the **wlng.datasource** select **Oracle's driver (Thin XA) for Instance connections**
  - For **wlng.localTX.datasource** select **Oracle's driver (Thin) for Instance connections**
  - Also be sure to select the correct driver during domain configuration.
- Oracle 12c PDB databases uses these datasources:
  - For the **wlng.datasource** select **Oracle's driver (Thin XA) for Service connections**
  - For the **wlng.localTX.datasource** select **Oracle's driver (Thin) for Service connections** as listed in Table 1–1.

Table 1–1 Oracle Database Connections

Database	wlng.datasource Driver to Use	wlng.localTX.datasource driver to use	Recommened Connection URL
Oracle 12c PDB	oracle.jdbc.xa.client.OracleXADataSource	oracle.jdbc.OracleDriver	**jdbc:oracle:thin:@//***host_ip*:*port*/*service_name*
Oracle 12c CDB	oracle.jdbc.xa.client.OracleXADataSource	oracle.jdbc.OracleDriver	**jdbc:oracle:thin:@***host_ip*:*port*:*service_id*
Oracle 12 non-CDB versions	oracle.jdbc.xa.client.OracleXADataSource	oracle.jdbc.OracleDriver	**jdbc:oracle:thin:@***host_ip*:*port*:*service_id*
Oracle 11g	oracle.jdbc.xa.client.OracleXADataSource	oracle.jdbc.OracleDriver	**jdbc:oracle:thin:@***host_ip*:*port*:*service_id*

New and Changed Features in Release 6.1 Patchset 1

The features in this section were added to Services Gatekeeper in a patch after the first version of the 6.1 release shipped.

New MySQL/Oracle Database Options for Single-Tier Services Gatekeeper

You can now use the single-tier version of Services Gatekeeper with the MySQL or Oracle 12c databases. See (Optional) Installing a Different Database in *Services Gatekeeper Getting Started Guide* for details.

The JavaDB Port is Now Configurable

The single-tier installation GUI page now offers you the chance to change the default JavaDB port. It displays the default port, 1547, which you can change to any port number you use.

New Enhancements to the Json2Xml Action

The Json2Xml API management action now:

- Offers the **instanceid**, **Default Name Space**, and **Root Tag** attributes. See Json2Xml in *Services Gatekeeper API Management Guide* for details.
- Supports moving data directly from the request input stream to the output stream. See Common Actions Programming Tasks in *Services Gatekeeper API Management Guide* for details.

New and Changed Features in Release 6.1

The features in this section were added in this release of Services Gatekeeper.

New Access URLs for the PRM Portals

You now access the portals by using these new URLs:

- Partner and API Management Portal:

  http://*IP_address*:*port*/**portal/partner-manager/index/login.html**

- Partner Portal:

  http://*IP_address*:*port*/**portal/partner/index/partnerLogin.html**

- Network Service Supplier Portal:

  http://*IP_address*:*port*/**portal/service-supplier/index/ssLogin.html**

The old URLs were:

- **http://***IP_address*:*port*/**partner-manager/index/login.html**
- **http://***IP_address*:*port*/**partner/index/partnerLogin.html**
- **http://***IP_address*:*port*/**service-supplier/index/ssLogin.html**

New Ability to Add Your Own Custom Actions for APIs

You can now create your own custom Actions to add to the Partner and API Management portal for use by all your APIs. In previous releases, you could apply custom code to the Groovy action, but you were required to propagate that code across all APIs. Custom actions that you create are available to all your APIs. See "Creating Custom Actions for Your APIs" in *Services Gatekeeper Portal Developer's Guide* for details.

IPv6 Mapping No Longer Required

In previous releases, using IPv6 addresses when configuring domains required that you create a mapping file. This step is no longer required. Instead, add the IPv6 addresses to the configuration GUI in square brackets "[]" when configuring domains.

New Actions and Features Available for API Actions

This section lists the new features available as actions for your APIs.

New System Performance Settings for Actions

These performance settings have been added to make Actions processing more efficient:

- **KeepNorthSession**
- **EnableSouthCookie**
- **UseSession**
- **MaxTotalConnections**
- **SocketTimeoutMS**
- **ReuseAddress**

See "Administering Actions Performance Settings" in *Services Gatekeeper API Management Guide* for details.

Set System Performance Settings Using the WebLogic Startup Script

These actions system performance settings are now available for you to use globally when you start the Services Gatekeeper server using the **-D** option to the startup script:

- oracle.sdp.daf.max_total_connections
- oracle.sdp.daf.socket_timeout_ms
- oracle.sdp.daf.connect_timeout_ms

See "Using the WebLogic Startup Script to Set Action System Performance Settings" in *Services Gatekeeper API Management Guide* for details.

Support for CORS Security for APIs

Support for browser Cross-Origin Resource Security (CORS) has been added to the Services Gatekeeper API management features as an API action. You use this action to direct a browser to accept resource calls for an API from servers in different domains. Browsers typically prohibit cross-domain resource sharing for security reasons. However, the system hosting your API may be on a different domain from the server hosing the API client, and they may need to share resources.

For example, a browser running on a remote system connecting to an API client on a web site in one domain, needs to call resources from the API hosted on another domain. The CORS feature allows you specifically allow the interaction between the browser and these two web sites while disallowing all others. The action is available as a middle action in the request message action chain. See "About the Default Actions" in *Services Gatekeeper API Management Guide*, and the *API and Partner Manager Online Help* for details.

New Security Validation for Groovy Action Scripts

The **Groovy** action now validates Groovy scripts before they are allowed to run in Services Gatekeeper. For a list of Java and Groovy components that are no longer allowed, see "Prohibited Components in Groovy Actions" in *Services Gatekeeper API Management Guide*.

> **Note:** You need to confirm that your Groovy scripts from previous releases pass validation by Services Gatekeeper.

New Ability to Limit Access to a Specific API Endpoint

The **RateLimit** API action has been added in this release that you use to limit the number of requests allowed for a specific API URI during a configurable time period. This new action applies to HTTP-to-HTTP communication requests to a specific URI. You can set multiple **RateLimit** actions to further refine this access.

For more information, see "Actions Provided by Services Gatekeeper" in *Services Gatekeeper API Management Guide* and *Services Gatekeeper API and Partner Management Portal Online Help*.

New Ability to Identify Actions with Instance ID Parameter

A new Instance ID parameter has been added to all of the default Actions. This field allows you to create a informal versioning system for your actions. The instance ID value appears in the EDRs that show action processing. See "Understanding the Default EDR fields for API Management" in *Services Gatekeeper System Administrator's Guide* for details on how this field appears in EDRs, and *Services Gatekeeper Partner and API Management Portal Online Help* for details on how to configure this field.

New Action to Authenticate Applications Using Application Key

The **AppKeyAuthentication** action has been added to the actions available for use on API traffic. It overrides the default behavior when using an application key to authorize API traffic to use a Services Gatekeeper API method. See "Actions Provided by Services Gatekeeper" in *Services Gatekeeper API Management Guide* and in the *Services Gatekeeper Partner and API Management Portal Online Help* for details.

To support this action, the API **application** object now contains **appKey** and **clientId** fields. Use the application management operations in the API Management REST-based API to create and manipulate application objects. Normally they are set by a partner. However, if the automatic approval settings for the Partner and API Manager Portal are on, the partner manager role can also set them.

Use the **getAppByClientID** operation to the **ApplicationStoreHelper** MBean to retrieve **appKey** object field value. See the "All Classes" section of the *Services Gatekeeper Java API Reference* documentation for information on **ApplicationStoreHelper**.

New API Management Options for Securing the Services Gatekeeper Methods

New in this release, Services Gatekeeper offers expanded options for authorizing applications to use the Services Gatekeeper API methods. You make this selection when you create each API using the Partner and API Management Portal. The **Exposed API Security** options allow you to use a combination of text-based and OAuth authorization, or use an application key (sometimes called an API key). If you use the application key option, Services Gatekeeper checks the query parameter first,

then the header for the key. You can override this option using the **AppKeyAuthorization** action.

New Ability to Protect REST APIs with a While List of IP Addresses

New in this release, you have the ability to protect REST-based APIs by creating a list of IP addresses that are solely allowed to communicate with the Services Gatekeeper application tier (AT). You use a special key/value pair created for the **updateAllSysConfig** operation to create the list. See "Protecting REST APIs with a White List of IP Addresses" in *Services Gatekeeper Security Guide* for details.

New Option to Create an API Without Authentication

In some cases automatic authentication is impractical for APIs, and new in this release you can create an API without a default authentication method. You can also authenticate it using an application key. See "New Action to Authenticate Applications Using Application Key" for a description.

New EDR/Alarm for ApiFirewall Violations

New in this release, the **CreateViolationEdrs** attribute has been added to the **ApiFirewallMBean**. This attribute is boolean, and the default value is true. In the event of a firewall violation, it creates an EDR and alarm for the violation.

See "Configuring Network Traffic Security with ApiFirewallMBean" in *Services Gatekeeper Security Guide* for details.

API Management Now Accepts HTTP Delete Actions

In the Services Gatekeeper 6.0 release, the API management features did not allow RESTful HTTP DELETE operations on backend services. This has been changed and DELETE actions are now supported for use with API management.

New Clarification on Using Variables and Wildcards for API Resource Mapping

The new "About Presenting APIs to Your Customers" section in *Services Gatekeeper API Management Guide* clarifies the mapping scheme that you can use to map the URLs in request messages to the URIs of actual API resources or services. This mapping allows you to create a different internal URL structure for your API services than you present to customers. This is particularly useful for REST-based communication, and allows you to change your internal URI scheme without requiring customers to change their existing request messages.

New Subscription Management Features

These new subscription management features are available for use with communication services:

- Changes to the **loadAppSubscriptionsXml** operation of the **SubscriptionPluginMBean**:
  - **expirePeriod** has been added. It scans for expired subscriptions. Set in minutes.
  - **subscribeInfo.notification** is now optional. In previous releases it was mandatory.

  - **unsubscriptInfo.notification** is now optional. In previous releases it was mandatory.
  - **suspendInfo.notification** is now optional. In previous releases it was mandatory.
  - **unsuspendInfo.notification** is now optional. In previous releases it was mandatory.
- The **loadAppSubscriptionsXml** operation now also includes the **appendingExpirePeriod** parameter.
- Subscription operations are now atomic.
- Subscription expiration behavior has changed. Services Gatekeeper now checks whether the subscription has expired each time it receives a retrieval request.

See "Application Subscription Management" in *Services Gatekeeper Communication Service Reference Guide* for information on subscription management.

New Option to Create Applications Without APIs

New in this release, Partners can use the Partner Portal to create applications without first subscribing to an API. Partners have the option to subscribe APIs to applications after the application has been created and approved by the partner manager.

New Ability to Use 24- and 32-Byte Application Passwords

New in this release, Services Gatekeeper now takes advantage of the Java Cryptography Extension (JCE) features to allow you to use 24- and 32-byte passwords to protect applications. See "Encrypting Application Passwords" in *Services Gatekeeper Security Guide* for instructions.

EDR Enhancements for API Management

This section lists the EDR enhancements that have been added since the last documentation reposting. See "Managing and Configuring EDRs, CDRs, and Alarms" in *Services Gatekeeper System Administrator's Guide* for details these new features.

New EDR Fields for API Management Processing

These fields have been added to Services Gatekeeper event data records (EDRs) for API management traffic (they do not apply to communication service traffic):

- **ApiId** - The API ID.
- **ApplicationId** - The application identifier
- **ErrCat** - Error category. Can be one of: ActionErr, ServiceErr, or PeerErr.
- **HttpStatusCode** - The response message HTTP status code.
- Time stamps before and after access tier, network tier, or network processing. For example **TsAfNET** (time stamp after network).
- **RspMsgSize** - Request Message Body Size
- **ReqMsgSize** - Response Message Body Size
- **ReqAction** - A record of all actions executed against a request message.
- **RspAction** - A record of all the actions executed against a response message.
- **Status** - The final HTTP status of the response message.

- **URL** - The service URI.

New Ability to Persist EDRs Until JMS Listeners Are Available

A new setting to the Services Gatekeeper domain **Time-to-live Override** parameter allows you to persist EDRs until Java Messaging Service (JMS) listeners are available to receive them. This is useful to capture information before the JMS listeners are created or available. For details on changing this setting, see "Managing and EDR, CDR, and Alarm Processing" in *Services Gatekeeper System Administrator's Guide*.

New EDR Partitioning Feature for API Management

An "EDR partitioning" feature has been added to Services Gatekeeper that groups related EDRs together and then sends them as a group to a single JMS listener. The default behavior (replicated EDRs) sends all EDRs to all listeners, which can cause confusion.

Services Gatekeeper does this by indexing EDR records with a JMS unit of order (UOO) value, and then grouping EDRs with the same UOO together. Then periodically it sends these groups to the appropriate JMS listener. That way, individual JMS listeners only receive a subset of EDR records. The default condition does not use EDR partitioning so you must configure this feature. For details, see "Managing and Configuring EDRs, CDRs, and Alarms" in *Services Gatekeeper System Administrator's Guide*.

New Functionality for APIs

This section lists new and improved features for Services Gatekeeper APIs.

New Ability to Suspend Applications for an API

New in this release is the ability to quickly and easily prevent an application from using an API. A new **Suspend/Un-Suspend** button has been added to the **Applications** tab for each API. Clicking this button allows/disallows the application from using the API. A notification is sent to the Partner Portal each time you click this button.

New API Identifier Added to Create Custom Access URLs

New in this release, the APIs you create now have two identifiers. Instead of just an API name, each API now has a *display name* (the old name) and a new *context root* that is appended to the Access URL for the API. This change allows you to create a custom API name for use in the PRM Portals that is different from the name used in the access URL.

You are not required to enter both identifiers however. If you fill in just one of the fields, that value is used for both the name and context root.

Previously, an API name of **WeatherAPI** and version of 1 required you to use this Access URI:

`http://IP_Address:port:/daf/WeatherAPI/1`

You now can use a different context root to customize the API access URL for your customers. For example, if specify WeatherAPI as name, and use **WeatherSouthWestAPI** as the context root, and omit the version number, you can present you customers with this access URI:

`http://IP_Address:port/WeatherSouthWestAPI`

Note that the **/daf** prefix is also no longer used; the version number in the access URI is now optional; and within Services Gatekeeper the API is still named **WeatherAPI**.

The object field for the API name is **apiName**, and the object field for the context root is **apiDisplayName**.

You change the context root using the new **editAPIContextRoot** operation to the Actions REST API.

See "About Naming and Presenting APIs to Your Customers" in *Services Gatekeeper API Management Guide* and the *Services Gatekeeper Partner and API Management Portal Online Help* for more information. Also see **editAPIContextRoot** in *Services Gatekeeper Portal Developer's Guide*.

/daf Prefix Removed from API Access URIs and EDRs

In previous releases, you were required to include `/daf` in the syntax for the API Access URL when you created an API in the Partner and API Manager Portal. This requirement has been removed.

The new syntax:

`http://IP_addr:port_no/api_name/version_no`

The old syntax:

`http://IP_addr:port_no/daf/api_name/version_no`

This change is also reflected in the EDR URL field. It no longer contains the **/daf** prefix for the API URL.

This EDR identifier:

`url:/daf/`*`api_name`***`/`***`version`*

changes to:

`url:/`*`api_name`***`/`***`version`*

New Flexibility for Versioning APIs

You can now choose to use no versioning for specific APIs that you create. You can simply leave the **Version** field blank when creating the API. The Access URL then does not show a version value.

Support for the New Diameter Timestamp Data Type - May Require that You Update Your Code

The Diameter specification has changed with regard to the timestamp data type. The old Diameter data type that previous releases of Services Gatekeeper supported defined a Diameter timestamp as an integer (seconds since from the start of the year 1970). Services Gatekeeper now supports the newer Diameter stack (version 6.3.0.1 and later) that defines a timestamp as **Type.TIME_BYTES** (number of seconds since the start of the year 1900). This type acts like a byte buffer, but limits the length of the buffer to 4 bytes.

> **Note:** If you use the Services Gatekeeper Diameter payment features, you need to update your code to use this new timestamp data type, and then test to be sure that the result is what you expect.

New Non-Standard Diameter Rx AVP Support for QoS Features

Services Gatekeeper now supports these Diameter Rx AVPs to implement with QoS features. These AVPs are not included in the Diameter Rx 3GPP TS 29.214 Specification, but are supported by Services Gatekeeper.

- FramedPort - for Rx AAR messages
- requiredAccessInfo - for Rx AAR messages
- endUserOpaqueId - for Rx AAA messages
- msTimeZone - for Rx AAAmessages
- userLocationInfo - for Rx AAA messages
- apnAMBRUL - for Rx AAA messages
- apnAMBRDL - for Rx AAA messages

See "Non-Standard Supported Diameter AVPs" in *Services Gatekeeper Statement of Compliance* for details on these AVPs.

New Support for JavaDB with Multi-tier Services Gatekeeper

The Oracle JavaDB database is now supported for use with multi-tier implementations of Services Gatekeeper. Specifically, this database is appropriate for testing and smaller production implementations. JavaDB is embedded in Services Gatekeeper so you do not have to obtain it separately. If security and performance are not issues, you can also install this database on the same physical system as the Services Gatekeeper Administration server and managed servers. See “Database Planning” and “Installing JavaDB Software” in *Services Gatekeeper Multi-tier Installation Guide* for details on installing this database.

New Custom Native SMPP Error Code for Custom Interceptors

It is now possible to specify a custom SMPP errorcode to be used with **SubmitSmResp/SubmitSmMultiResp** methods. The new error code is designed to be sent back to a Native SMPP client in cases where the **SubmitSm/SubmitSmMulti** action is rejected by a custom interceptor.

If the custom interceptor wants to reject the **SubmitSm/SubmitSmMulti** request, it can specify the SMPP command status to send back to the Native SMPP client by throwing a **DenyPlugin** Exception created on this form:

```
new_DenyPluginException("custom_smpp_errorcode", <smpp commandstatus in decimal form>)
```

For example if the interceptor throws a new **PluginDenyException("***custom_smpp_errorcode***", 123)**; the **SubmitSmResp/SubmitSmMultiResp** sends the 0x0000007b (hex 7b = 123 decimal) command status back to the Native SMPP client.

New Attributes for Native SMPP MO Messages

These MBean attributes have been added to the Native SMPP communication service MBean (**SMPPServiceMBean**) to process mobile-originated messages:

- **rejectMOMessagesWithNoAppReceiverConnection**

  Mobile-originated native SMPP communication service requests are successful only if Services Gatekeeper has a connection to both a receiver (SMSC), and an application that accepts **DeliverSm**. The default behavior is to reject any request

that does not have these two connections, but the message is processed by the interceptor stack before probing for the Services Gatekeeper-application connection

If the new attribute is set to TRUE, Services Gatekeeper probes for the application connection *before* the interceptor stack, which is faster and more efficient than the default behavior.

SMPP mobile originated connection errors generate alarm 400514. See "400514 SMPP Server Service: MO Request Failed" in *Service Gatekeeper Alarms Handling Guide* for details.

- **native_smpp_mo_destAddressHasAppMapping**

  This attribute is checked at the MO_SOUTH interception point.

  If TRUE an application matching the destination address in **DeliverSm** exists.

  If FALSE, no application matching the destination address is in **DeliverSm**.

- **native_smpp_mo_hasActiveReceiver**

  This attribute is only be checked at the MO_NORTH interception point.

  If TRUE, the application has an active receiver connection.

  If FALSE, the application has no active receiver connection.

See "Native SMPP" in *Services Gatekeeper Communication Services Reference Guide* for details on this communication service.

Known Issues

This section lists the known issues in this release of Services Gatekeeper.

Database Rollback Issue for Later Patchsets

After upgrading, if you need to rollback your Services Gatekeeper implementation, the database schema automatically reverts to the 6.0 + patchset 2 level.

See "Upgrade Restrictions" in *Services Gatekeeper Multi-tier Installation Guide* for details on this issue.

Message Payload Size Limitation

The maximum message payload size for the Dynamic Application Programming Interface Framework (DAF) that handles HTTP to HTTP traffic is **200 MB**.

Known Issues

Table 1–2 lists the other known issues in this release.

Table 1–2 Known Issues in this Release

Bug ID	Description
24570293	Using **oneApiSendSms** to send an SMS message using an **EncodType** of **URLEncode**, and an empty username fails and returns this error: `{"requestError":{"serviceException":{"messageId":"SVC0001", "text":"A service error occurred. Error code is %1","variables":["Not support oneAPI binary message!"]}}}` Be sure to add a non-empty username to send the SMS.

24496485	Using a single-tier Services Gatekeeper with MySQL version 5.7.14 requires this workaround:
	1. Download **mysql-connector-java-5.1.39-bin.jar** from
	`https://dev.mysql.com/downloads/connector/j/`
	2. In *Gatekeeper_home*/**oracle_common/modules/** rename the **mysql-connector-java-commercial-5.1.22-bin.jar** file as a backup copy.
	3. Move the file you downloaded in Step 1 to *Gatekeeper_home*/**oracle_common/modules/**
	4. Rename the file to **mysql-connector-java-commercial-5.1.22-bin.jar**.
	5. (If you prohibit SSL JDBC connections) In *domain_home*/**config/jdbc/** add this entry to the **wlng-localTX-jdbc.xml** and **wlng-jdbc.xml** files:
	`<property>`
	`<name>useSSL</name>`
	`<value>false</value>`
	`</property>`

24487406	Starting an Services Gatekeeper AT server can sometimes return this error message: `<Warning> <DeploymentService> <BEA-290064> <Deployment service servlet encountered an exception while handling the deployment service message for request id "-1" from server "WLNG_AT1". Exception is: "java.io.OptionalDataException` This error message is spurious and you can safely ignore it.
24471711	Occasionally, starting a Services Gatekeeper managed server returns this error message: `<Error> <Cluster> <BEA-003122> <ORA-00942: table or view does not exist: A cluster that has migratable servers could not create/execute SQL statement when validating the database connection. The cluster is misconfigured. Check the leasing table on the database and connection configuration.>` This error message is spurious and you can safely ignore it.
24322135	An API application ID is changed by Services Gatekeeper when a partner manager removes the API. If you created an API with a custom application ID, this ID is temporarily changed when a partner removes the application using the API. The correct application ID is returned when the partner manger approves the remove application operation.

Table 1–2 (Cont.) Known Issues in this Release

Bug ID	Description

20116778	When creating a clustered single-tier Services Gatekeeper implementation, the second clustered system sometimes returns this error message:
	`Replicated call`
	`state manager could not initialize all partitions'`
	
	and this status message
	`<New view for partition part-1: Partition viewId=0 Name=part-1 CreatingReplicaId:Name=0:Node1 Replicas=[0:Node1]>`
	
	These messages are spurious and you can be safely ignore them.

Documentation Corrections and Additions

This section lists errors in the Services Gatekeeper documentation.

Understanding the API Management Proxy Settings

These options determine the proxy settings that your APIs use. They are enforced in this order (the last one wins):

1. The Java operating system proxy settings (**http.proxyHost**, **http.proxyPort**, **https.proxyHost**, and **https.proxyPort**).

   See the Java documentation for instructions on how to configure these settings.

2. The proxy server that you enter in the **Network Proxy** field in each API.

   See *Services Gatekeeper Partner and API Management Portal Online Help* for information on using this field.

3. Creating a proxy object in a **Groovy** action in each API.

   See "Using Actions to Manage and Manipulate API Traffic" in *Services Gatekeeper API Management Guide* for details on the actions you can create for each API.

Understanding API HTTP/HTTPs Proxy Access

The **Network Proxy** *ip_address*:*port* entry that each API can use supports both http and https API service URLs. For example, set **Network Proxy** to **cn-proxy.jp.mydomain.com:80**:

- If you specify an http service URL, the resulting proxy setting is **http.proxyHost=cn-proxy.jp.mydomain.com**, **http.proxyPort=80**
- If you specify an https service URL, the resulting proxy setting is **https.proxyHost= cn-proxy.jp.mydomain.com**, **https.proxyPort=80**

Setting the EDR Types to Send to EdrService

These descriptions for the EDR types were inadvertently left out of the documentation set. These settings determine what types of EDRs are sent out from **EdrService**

- **publish_programmable_edr** (Boolean) - Default: **true**. Sends out EDRs created manually by **EdrDataHelper**. These EDRs do not have a **state** attribute.

- **publish_facade_edr** - (Boolean) - Default: **false**. Sends out EDRs created in the AT. The state is either **ENTER_AT** or **EXIT_AT.** The default is **false** because all of these EDRs are created for EDR analytic already.
- **publish_enabler_edr** - (Boolean) - Default: **true**. Sends out EDRs with a state of either **ENTER_NT** or **EXIT_NET**.
- **publish_protocalStack** - (Boolean) - Default: **true**. Sends out EDRs with a state of either **ENTER_NET**, or **EXIT_NT**.
- **publish_others_edr** - (Boolean) - Default: **true**. Sends out all other EDRs; they do not have a state attribute, however their **interface** is set to **other**.

When Services Gatekeeper is in EDR analytic mode, be sure the change these settings to:

- **publish_programmable_edr** - false
- **publish_facade_edr** - true
- **publish_enabler_edr** - true
- **publish_protocalStack** - true
- **publish_others_edr** - false

You use the Administration Console (**OCSG**, then *servername*, then **Container Services**, then **Attributes**), or **EdrServiceMBean** in the *OAM Java API Reference* to change these settings. See "When EDRs are Generated" in *Services Gatekeeper System Administrator's Guide* for more information on EDRs and EDR states

Client HTTP Headers Not Passed to Your Network Service

Services Gatekeeper automatically passes all HTTP headers from an application (client) to your network service, except the those listed in this section. If your network service requires them, you can create a Groovy action that gets them from the incoming message, and sets them on the outgoing message.

- **Proxy-Authorization**
- **Authorization**
- **Content-Length**
- **Transfer-Encoding**
- **Transfer-Encoding**
- **Host**
- **OCSGOAuthBearer**
- **OCSGOAuthMAC**
- **Anonymous**
- **OCSGProxy-Authorization**
- **OCSGSoapHeader**
- **OCSGAppKeyHeader**

The information in these sections will help you create the custom groovy action:

- "Printing and Changing Message Content" in *Services Gatekeeper API Management Guide*.

- "Creating Custom Actions for Your APIs" in *Services Gatekeeper Portal Developer's Guide*.

Implementing a Backend Service Protected by HTTPS

Services Gatekeeper supports exposing a Southbound URL secured with HTTPS, by first importing the required website certificate to the WebLogic server truststore.You add the required certificate to the WebLogic server truststore (**DemoTrust.jks** file) by running this **keytool** command from the *install_home***/wlserver/server/lib** directory:

```
keytool -import -alias myCa1 -trustcacerts -file $cert_file -keystore
DemoTrust.jks -storepass store_password
```

For example:

```
keytool -import -alias myCa1 -trustcacerts -file $myCertFile -keystore
DemoTrust.jks -storepass trustme199
```

See "Configuring Keystores" and "Keytool Command Summary" in *Fusion Middleware Administering Security for Oracle WebLogic Server* for general information on creating keystores and details on the **keytool** command.

Incorrect Filenames for Creating Custom Actions

The "Creating and Adding a Custom Actions to Services Gatekeeper" section in *Services Gatekeeper Portal Developer's Guide* contains references to the wrong files in step 5. The correct files to add to your Java compiler CLASSPATH are:

- *Gatekeeper_home***/ocsg/dynamic-action/oracle.sdp.registration.prs**_*release_level***.jar**.
- The **/WEB-INF/lib/oracle.sdp.daf-***release_level***-SNAPSHOT.jar** file in *Gatekeeper_home***/ocsg/applicatons/daf.war** (unzip the .war file).

Incorrect Name for OneAPI MMS Response Field

The "OneAPI Multimedia Messaging/MM7" chapter of the *Services Gatekeeper Communication Service Reference Guide* was based on an incorrect specification document. It erroneously specified the **deliveryInfoList** field instead of the correct **deliveryInfoNotification** field in OneAPI MMS delivery notification messages. The document has been corrected.

Corrections to How Sessions Operate with the validityTime Field

These additions to the description of the **getSessionRemainingLifeTime** operation to the **SessionManager** WSDL file were left out of the Services *Services Gatekeeper Application Developer's Guide*:

Operation: getSessionRemainingLifeTime

Returns the remaining lifetime of an established session in minutes. This operation works with the **validityTime** field in the **ApplicationSessionMBean**. The default value for **validityTime** is 0 minutes, which keeps the session open indefinitely unless you specially destroy it. You can change the default to set a time limit for all sessions. When the time limit expires, the session is automatically destroyed.

If **validityTime** is set to the default (**0** minutes), the session is always valid unless you destroy it. **getSessionRemainingLifeTime** returns these example values if you use the default **validityTime** value:

- Immediately after the session is created, this operation returns **0**.
- 1 minute after the session is created, this operation returns **-1**.
- 3 minutes after the session is created, this operation returns **-3**.

If you change the **validityTime** value to a positive number of minutes, this operation destroys the session at the end of that time period. For example if you set **validityTime** to **5** minutes, you get this behavior:

- Immediately the session is created, this operation returns **5**.
- 1 minute after the session is created, this operation returns **4**.
- 3 minutes after the session is created, this operation returns **2**.

  5 minutes after the session is created, it is invalidated and destroyed.

See the "All Classes" section of the *Services Gatekeeper OAM Java API Reference* for details on **ApplicationSessionMBean**.

Input message: getSessionRemainingLifeTime
Table 1–3 Input Message: getSessionRemainingLifeTime

Part name	Part type	Optional	Description
sessionId	xsd:string	N	The ID of an established session.

Output message: getSessionRemainingLifeTimeResponse
Table 1–4 Output Message: getSessionRemainingLifeTimeResponse

Part name	Part type	Optional	Description
getSessionRemainingLifeTimeReturn	xsd:string	N	The remaining lifetime of the session. Given in milliseconds.

Referenced faults None

2

Database Schema Changes

This chapter lists the database schema changes between Services Gatekeeper 6.0 and Services Gatekeeper 6.1.

New Database Tables

The following database tables are new in this release. The column names are listed in ascending order.

prm2_daf_actionAPIMap

Table 2–1 lists the columns in the new table, **prm2_daf_actionAPIMap**, added in this release.

Table 2–1 prm2_daf_actionAPIMap Table

New Column Name	Data Type
ACTIONNAME	VARCHAR2(512
APIID	VARCHAR2(100)
APINAME	VARCHAR2(100)
STORED_TS	NUMBER(38)

endpoint_authentication_config

Table 2–2 lists the columns in the new table, **endpoint_authentication_config**, added in this release.

Table 2–2 endpoint_authentication_config Table

New Column Name	Data Type
CONFIG	BLOB
CONTEXTROOT	VARCHAR2(255)
STORED_TS	NUMBER(38)

Updated Database Tables

The following database tables were updated for this release:

- oauth2_access_token
- oauth2_authorization_code

- oauth2_client
- oauth2_refresh_token
- oauth2_resource_owner
- pl_payment_reservation_data
- pl_payment_volume_reservation
- prm2_api_actions
- prm2_app_apis_methods
- prm2_application
- prm2_apis
- prm2_daf_actions
- rest_qos_session_data
- south_oauth2_client
- wlng_internal_subscriber

The column names are listed in ascending order.

oauth2_access_token

Table 2–3 lists the updated **oauth2_access_token** table.

Table 2–3 oauth2_access_token Table

New Column Name	Data Type
ACCESS_TOKEN	VARCHAR2(64)
APPINSTANCE_ID	VARCHAR2(100)
CLIENT_ID	VARCHAR2(100)
EXPIRED_TIME	NUMBER(38)
INVOKE_COUNT	NUMBER(38)
ISSUE_TIME	NUMBER(38)
MAC_ALGORITHM	VARCHAR2(40)
MAC_KEY	VARCHAR2(20)
NONCE_AGE	NUMBER(38)
NONCE_RANDOM	VARCHAR2(128)
PARAMETER	VARCHAR2(512)
RESOURCE_OWNER	VARCHAR2(128)
RESOURCE_SCOPE	VARCHAR2(4000)
STATE	VARCHAR2(512)
STORED_TS	NUMBER(38)
TOKEN_TYPE	VARCHAR2(32)

oauth2_authorization_code

Table 2–4 lists the updated **oauth2_authorization_code** table.

Table 2–4 oauth2_authorization_code Table

New Column Name	Data Type
ACCESS_TOKEN	VARCHAR2(64)
CLIENT_ID	VARCHAR2(100)
CODE	VARCHAR2(64)
EXPIRED_TIME	NUMBER(38)
PARAMETER	VARCHAR2(512)
REDIRECT_URI	VARCHAR2(128)
REFRESH_TOKEN	VARCHAR2(64)
RESOURCE_OWNER	VARCHAR2(128)
RESOURCE_SCOPE	VARCHAR2(4000)
RESPONSE_TYPE	VARCHAR2(32)
STATE	VARCHAR2(32)
STORED_TS	NUMBER(38)

oauth2_client

Table 2–5 lists the updated **oauth2_client** table.

Table 2–5 oauth2_client Table

New Column Name	Data Type
ALLOWEDREDIRECTIONURIS	VARCHAR2(4000)
APPINSTANCEID	VARCHAR2(100)
CLIENT_ID	VARCHAR2(100)
CLIENT_SECRET	VARCHAR2(64)
DESCRIPTION	VARCHAR2(255)
NAME	VARCHAR2(100)
STORED_TS	NUMBER(38)
SUPPORTIMPLICITGRANT	NUMBER(38)

oauth2_refresh_token

Table 2–6 lists the updated **oauth2_refresh_token** table.

Table 2–6 oauth2_refresh_token Table

New Column Name	Data Type
ACCESS_TOKEN	VARCHAR2(64)
CLIENT_ID	VARCHAR2(100)
EXPIRED_TIME	NUMBER(38)
PARAMETER	VARCHAR2(512)
REFRESH_TOKEN	VARCHAR2(64)
RESOURCE_OWNER	VARCHAR2(128)

Table 2–6 (Cont.) oauth2_refresh_token Table

New Column Name	Data Type
RESOURCE_SCOPE	VARCHAR2(4000)
STORED_TS	NUMBER(38)

oauth2_resource_owner

Table 2–7 lists the updated **oauth2_resource_owner** table.

Table 2–7 oauth2_resource_owner Table

New Column Name	Data Type
ADDRESS	VARCHAR2(255)
ANONYMOUS_ID	VARCHAR2(64)
FROMRESOURCERULE	NUMBER(38)
RESOURCE_SCOPE	VARCHAR2(4000)
STORED_TS	NUMBER(38)

pl_payment_reservation_data

Table 2–8 lists the updated **pl_payment_reservation_data** table.

Table 2–8 pl_payment_reservation_data Table

New Column Name	Data Type
APP_ID	VARCHAR2(255)
CURRENCY	VARCHAR2(3)
EXPIRATIONTIME	NUMBER(38)
OWNER	VARCHAR2(255)
REFERENCESEQUENCE	NUMBER(38)
REQUESTEDAMOUNT	VARCHAR2(255)
REQUESTNUMBER	NUMBER(38)
SERVICECONTEXTID	VARCHAR2(255)
SESSIONID	VARCHAR2(255)
SP_ID	VARCHAR2(255)
STORED_TS	NUMBER(38)
SUBSCRIPTIONID	VARCHAR2(255)
USEDAMOUNT	VARCHAR2(255)

pl_payment_volume_reservation

Table 2–9 lists the updated **pl_payment_volume_reservation** table.

Table 2–9 pl_payment_volume_reservation Table

New Column Name	Data Type
APP_ID	VARCHAR2(255)

Table 2–9 (Cont.) pl_payment_volume_reservation Table

New Column Name	Data Type
BILLING_TEXT	VARCHAR2(255)
ENDUSERID	VARCHAR2(255)
EXPIRATIONTIME	NUMBER(38)
OWNER	VARCHAR2(255)
REFERENCESEQUENCE	NUMBER(38)
REQUESTEDVOLUME	NUMBER(38)
REQUESTNUMBER	NUMBER(38)
SERVICECONTEXTID	VARCHAR2(255)
SESSIONID	VARCHAR2(255)
SP_ID	VARCHAR2(255)
STORED_TS	NUMBER(38)
USEDVOLUME	NUMBER(38)

prm2_api_actions

Table 2–10 lists the updated **prm2_api_actions** table.

Table 2–10 prm2_api_actions Table

New Column Name	Data Type
ACTIONCHAINVER	NUMBER(38)
APIID	VARCHAR2(100)
REQACTIONS	BLOB
RESACTIONS	BLOB
SERVICEURI	VARCHAR2(100)
STORED_TS	NUMBER(38)

prm2_app_apis_methods

Table 2–11 lists the updated **prm2_app_apis_methods** table.

Table 2–11 prm2_app_apis_methods Table

New Column Name	Data Type
APINAME	VARCHAR2(100
APPLICATIONID	VARCHAR2(100)
ID	VARCHAR2(128)
INTERFACENAME	VARCHAR2(100)
METHODNAME	VARCHAR2(100)
QTADAYS	NUMBER(38)
QTALIMIT	NUMBER(38)
QTALIMITEXCEEDOK	NUMBER(38)
REQLIMITGUARANTEE	NUMBER(38)

Table 2–11 (Cont.) prm2_app_apis_methods Table

New Column Name	Data Type
RTREQLIMIT	NUMBER(38)
RTTIMEPERIOD	NUMBER(38)
STORED_TS	NUMBER(38)
SUSPENDED	NUMBER(38)
TIMEPERIODGUARANTEE	NUMBER(38)
TYPE	NUMBER(38)

prm2_application

Table 2–12 lists the updated **prm2_application** table.

Table 2–12 prm2_application Table

New Column Name	Data Type
ADDITIONALINFO	VARCHAR2(500)
APPINSTANCE	VARCHAR2(200)
APPLICATIONNAME	VARCHAR2(100)
CLIENTID	VARCHAR2(200)
DESCRIPTION	VARCHAR2(500)
EFFECTFROMDATE	NUMBER(38)
EFFECTTODATE	NUMBER(38)
ICON	VARCHAR2(200)
ID	VARCHAR2(128)
LOCKSTATUS	NUMBER(38)
NEEDREAD	NUMBER(38)
PARTNERNAME	VARCHAR2(100)
QTADAYS	NUMBER(38)
QTALIMIT	NUMBER(38)
QTALIMITEXCEEDOK	NUMBER(38)
RTREQLIMIT	NUMBER(38)
RTTIMEPERIOD	NUMBER(38)
STATUS	NUMBER(38)
STORED_TS	NUMBER(38)
SUBMITDATE	NUMBER(38)

prm2_apis

Table 2–13 lists the updated **prm2_apis** table.

Table 2–13 prm2_apis Table

New Column Name	Data Type
ACCESSTYPE	NUMBER(38)

Table 2–13 (Cont.) prm2_apis Table

New Column Name	Data Type
ACCESSURL	VARCHAR2(200)
APIDISPLAYNAME	VARCHAR2(100)
APIID	VARCHAR2(100)
APINAME	VARCHAR2(100)
APIVERSION	VARCHAR2(50)
AUTHTOKEN	VARCHAR2(100)
AUTHTYPE	NUMBER(38)
CONTRACTCONTENT	BLOB
CONTRACTNAME	VARCHAR2(100)
CONTRACTVERSION	VARCHAR2(10)
CSOPTION	NUMBER(38)
CSSERVICETYPE	VARCHAR2(500)
DESCRIPTION	VARCHAR2(1000)
DIRECTION	NUMBER(38)
FACADE	VARCHAR2(100)
ICON	VARCHAR2(200)
LINK	VARCHAR2(1000)
NETWORKAUTHORIZATIONURI	VARCHAR2(200)
NETWORKCLIENTREDIRECTURI	VARCHAR2(200)
NETWORKPROXY	VARCHAR2(200)
NETWORKTOKENURI	VARCHAR2(200)
NORTHBOUNDWADLCONTENT	BLOB
PRIVILEGELEVEL	NUMBER(38)
PROTOCOL	VARCHAR2(200)
SERVICETYPE	VARCHAR2(100)
STATUS	NUMBER(38)
STORED_TS	NUMBER(38)
WADLCONTENT	BLOB

prm2_daf_actions

Table 2–14 lists the updated **prm2_daf_actions** table.

Table 2–14 prm2_daf_actions Table

New Column Name	Data Type
APICONFIGURATION	BLOB
APIID	VARCHAR2(100)
SERVICEURI	VARCHAR2(100)
STORED_TS	NUMBER(38)

rest_qos_session_data

Table 2–15 lists the updated **rest_qos_session_data** table.

Table 2–15 rest_qos_session_data Table Changes

New Column Name	Data Type
APPINSTGRPID	VARCHAR2(255)
DESTINATIONHOST	VARCHAR2(255)
DURATION	NUMBER(38)
ENDUSERID	VARCHAR2(255)
FEATURENAME	VARCHAR2(255)
NODEID	NUMBER(38)
PLUGINID	VARCHAR2(255)
REQUESTID	VARCHAR2(255)
SESSIONDATA	BLOB
SESSIONID	VARCHAR2(255)
STORED_TS	NUMBER(38)

south_oauth2_client

Table 2–16 lists the updated **south_oauth2_client** table.

Table 2–16 south_oauth2_client Table

New Column Name	Data Type
ALLOWEDREDIRECTIONURIS	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(100)
DESCRIPTION	VARCHAR2(255)
STORED_TS	NUMBER(38)

wlng_internal_subscriber

Table 2–17 lists the updated **wlng_internal_subscriber** table.

Table 2–17 wlng_internal_subscriber Table

New Column Name	Data Type
ADDRESS	VARCHAR2(255)
ATTRIBUTE_MAP	BLOB
LOGIN_ID	VARCHAR2(64)
SECRET	VARCHAR2(255)
STORED_TS	NUMBER(38)